



**Rita Katz
Director
SITE Institute**

**Testimony before
The Homeland Security Committee
Subcommittee on Intelligence, Information Sharing and Terrorism
Risk Assessment
United States House of Representatives**

“The Online Jihadist Threat”

written by

**Rita Katz
Director
SITE Institute**

&

**Josh Devon
Senior Analyst
SITE Institute**

November 6, 2007





The Internet: The Most Vital Tool for Terrorist Networks

More than six years after 9/11, the United States has done little to contest jihadists' use of the internet, arguably one of the most crucial tool that enables modern terrorist networks to exist. Jihadists use the internet to recruit, coordinate, communicate, raise financing, plot attacks, and even as a social network. Yet, after much interaction with government officials from several agencies, including the military as well as domestic law enforcement, it is clear that while the government understands that the internet is being used by jihadists, few steps have been made to study this phenomenon. It is clear by the ballooning influence of the internet in fostering a global insurgency against the West and its interests, the government lacks a full grasp of how jihadists exploit the internet, and even less of an idea on how to combat this threat effectively in a coordinated effort.

Today, there are tens of thousands of members on the half a dozen most important and exclusive online password-protected jihadist messageboards, and many more in line to take the place of those members who have used the internet to pave the way to kill themselves in suicide bombings in Iraq, Afghanistan, Somalia, Chechnya, and Lebanon. Likewise, as it has become more difficult to travel to current conflict areas for military instruction, the internet provides a virtual training camp for those members who seek to plan homegrown terrorist attacks in the United States and other Western targets. It is the internet that enables jihadist groups to foster a global insurgency, preparing like-minded individuals all over the world with the necessary military, technical, and social skills to produce a dangerous, united movement aimed at harming the West and Western interests.

Though labyrinthine, confusing, and requiring the in-depth study of complex social and technical networks, this essential battleground in combating the terrorist threat must be considered as important as fighting terrorists on the ground. Attempted homegrown terrorist attacks on the West have increasingly included an online component, whether the assailants were using the internet to coordinate the transfer of information, download military manuals, watch jihadist videos, or participate on jihadist messageboards. Of course, guns, IEDs, and other weapons are necessary for terrorists to maintain their relevance and dangerousness, but the internet is what enables jihadists to coordinate attacks, share information, recruit new members, and propagate their ideology. There is no longer any doubt that the internet is the heart of the global jihadist movement.

The government has attempted to monitor the internet by automatically analyzing huge amounts of online traffic through computers, which has led to positive results intercepting emails and other online communication related to terrorist activity. However, this method of data gathering misses crucial intelligence, especially as jihadists come up with novel ways to avoid automated detection online, and glosses over the critical nuances that comprise the online jihadist community, like their demographics, their geography, their ideology, and their manner of thinking.



As the SITE Institute and other private organizations have successfully been able to gather actionable intelligence from jihadists on the internet, not by using supercomputers but instead by knowing where and when to look, after having spent several years infiltrating, studying, and analyzing the online jihadist community. As just one example, after infiltrating and monitoring an online jihadist internet forum used for recruitment, the SITE Institute obtained intelligence that members of the forum were soon leaving their countries of residence in Europe to engage in suicide operations against coalition forces in conflict areas. The SITE Institute first alerted domestic law enforcement, who were unaware of the threat, and then contacted law enforcement officials in Europe, who determined that the intelligence was indeed actionable and promptly detained the individuals. This case, and others like it, are representative of how law enforcement agencies, in the United States and Europe, are not sufficiently monitoring the internet effectively.

Though necessary, rather than just using software to analyze massive flows of data hoping that a jihadist will use a key word like “bomb” in an email, the government also needs to focus its efforts on the much more difficult task of studying people to understand our enemy. This initiative involves a radical retraining of government analysts, who must at the same time be able to interpret and understand server logs, PHP, networks of IP addresses, and databases, in addition to a deep knowledge of jihadist culture and history, as well as foreign languages like Arabic, Turkish, Urdu, and Pashtu. Without the combination of these skills, which is what our enemies already possess, the United States will not be properly equipped to combat jihadists on the internet.

However, if the U.S. does cultivate these skills, it can deal severe blows to the global jihadist community. By effectively studying the internet, law enforcement and the military can learn about our enemy, including who they are, their location, their ideology, trends in tactics, and what training they are receiving. Understanding our enemy will help to counter their propaganda, predict types of future attacks, find them, and defend ourselves against their methods. Whether fighting groups of jihadists in Iraq or self-indoctrinated, homegrown terrorists in the United States, focusing on the internet puts law enforcement in the best possible position to combat the global jihadist threat.

Current Structure of the Online Jihadist Movement

In order to understand the global jihadist threat, it is necessary to review the structure of the online jihadist movement. After developing a basic knowledge of how jihadist groups utilize the internet, one can see how established jihadist groups like al-Qaeda direct the jihadist movement and can continue to exist despite the traditional measures taken against them. Once dissected, the online jihadist movement can be infiltrated, analyzed, and countered. The following provides an overview of how jihadists use the internet, how information is disseminated and circulated, and how the internet serves all the necessary functions jihadist groups need to continue to survive.

At least since the 1990s, Al-Qaeda and other jihadist groups have used the internet to broadcast

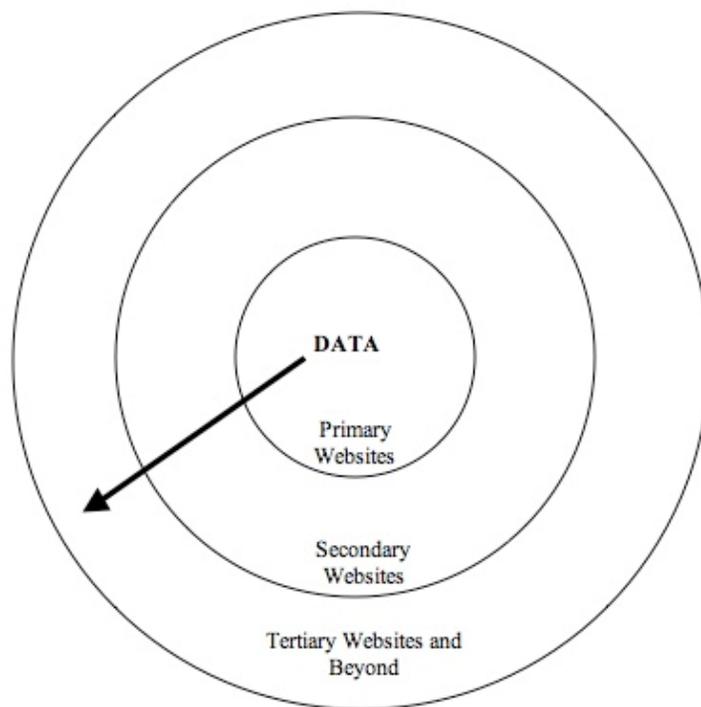


propaganda and recruit members. After 9/11 and the resulting destruction of terrorist training camps followed by the ensuing decentralization of al-Qaeda and other jihadist groups, the internet became essential to allowing jihadist groups to continue to operate effectively. Today, jihadist groups utilize websites, messageboards,¹ e-groups, blogs, instant messaging, and other services available through the internet to continue to indoctrinate, communicate, recruit, and plan attacks.

While many may perceive that jihadist activity on the internet is chaotic, it is in fact very structured. Only a handful of primary source jihadist websites distribute the media of the leaders of al-Qaeda and other jihadist groups. Through this small number of specific, password-protected online forums, the leading jihadist groups, like al-Qaeda, post their communiqués and propaganda. By keeping the number of primary source jihadist websites small, online jihadist ideologues and leaders of jihadist groups can provide a transparent mechanism to authenticate communiqués. In this way, the global jihadist movement can instantly discern the difference between official and fake communiqués by checking the source of the website and the individual who posted it. Though the number of primary source forums is small, there are tens of thousands of members registered on these websites, giving the jihadists a wide reach.

Once an official message from a jihadist group is posted to a primary source message forum, members of the primary message forum will then disseminate that posting to other secondary messageboards. From these secondary messageboards, other peripheral individuals will then disseminate the information onto other messageboards (See Figure Below)

¹ An online messageboard, also called an online forum, allows users to communicate and discuss topics easily with each other on the same website. Messageboards, which may be password-protected, foster the creation of virtual communities and are essential to reinforcing a shared global jihadist identify.



Dissemination of Primary Source Jihadist Data

Thus, the online jihadist movement has developed in such a way that it is at once decentralized but rigidly hierarchical. The jihadists can demonstrate that their communiqués are authentic by releasing information only on the primary websites and then rely on the secondary and tertiary websites to disseminate their data to larger groups of people.

Al-Fajr Center

The group that coordinates the online distribution of authentic jihadist communiqués, such as a video by bin Laden, Zawahiri, and other jihadist leaders, is called Al-Fajr Center. Established officially in January 2006, Al-Fajr Center is entirely virtual and exists only online. The organization serves not only al-Qaeda but numerous jihadist groups who share the same ideology. Besides al-Qaeda, the groups that utilize Al-Fajr Center include several of the Iraqi insurgency groups, Palestinian jihadist groups, Al-Qaeda in the Islamic Maghreb (formerly the GSPC), the Libyan Islamic Fighting Group, Somali jihadist groups, Saudi jihadist groups, the Taliban and other insurgent groups in Afghanistan, and even a group in western China.

The underlying purpose of Al-Fajr Center is to coordinate propaganda efforts through highly centralized and secure channels. This enables the groups utilizing al-Fajr to unify strategies, achieve economies of scale, and establish trusted channels of communication. Through the center's efforts, individuals across the globe are provided with easy access to authentic jihadist propaganda coming from a single source. This tactic slowly erases the lines between the regional terrorist groups, effectively portraying a strong, united group against the West. Because



of the apparent closeness between al-Qaeda and the other groups using Al-Fajr Center, those indoctrinated by Al-Fajr Center will support any jihadist group releasing media through the center, not just al-Qaeda.

The group's products are eclectic and very frequent, creating a stimulating environment for jihadists. Al-Fajr Center distributes dozens of daily communiqués from jihadist groups taking credit for attacks in Iraq, Afghanistan, Algeria, and elsewhere. In addition to these daily communiqués, the group also regularly dispatches special releases. For example, in November 2006, Al-Fajr released a written analysis of the current state of conflict in Afghanistan. The following week, the organization released a strategic manual, the "Technical Mujahid," devoted to understanding the internet and internet security. The very next day, the center was responsible for the release of a video provided by a representative of a Somali jihadist group. These releases came only days after a video calling for jihad in Xinjiang, China, called East Turkistan by the jihadists.

Al-Fajr Center itself is very structured and is divided into several different brigades, each with a designated purpose.

These brigades include:

- **Hacking Brigade**, in charge of hacking websites, carrying out Denial of Service (DoS) attacks, and identifying vulnerable websites
- **Intelligence Brigade**, in charge of gathering information, both online and in the physical world. For example, this brigade monitors the websites of the government, think tanks, and the media, like the White House, the U.S. Army, the Rand Corporation, the Jamestown foundation, Newsweek, Time Magazine, and others.
- **Distribution Brigade**, in charge of distributing the propaganda released by jihadist groups, such as taking credit for daily attacks, media from jihadist leaders, videos of attacks, training videos, and other videos of fighting from all over the world
- **Publications Brigade**, in charge of producing studies and training manuals in magazine form, like the "Technical Mujahid"
- **Cybersecurity Brigade**, in charge of protecting the security of jihadist websites
- **Multimedia Brigade**, in charge of producing multimedia jihadist propaganda, including attacks on American forces, preparation of IEDS, audio and video messages from jihadist leadership, statements of martyrs, and other propaganda

Each of these groups has its own special messageboard which only members of each brigade can access. Each brigade contains leaders who coordinate their efforts with the jihadist leadership. The costs to run these brigades are minimal, as those involved are donating their time and effort for their cause. The members of these brigades do their work not for any particular jihadist group but for the entire movement. The virtual layer between the members of these brigades and the actual jihadist groups themselves creates an extremely operationally secure mechanism to transmit information.



While these propaganda efforts are the driving force behind Al-Fajr Center, the organization does serve another purpose for jihadist groups by providing numerous services for jihadist leaders. Because Al-Fajr Center is in communication with representatives of all the major jihadist groups, including al-Qaeda, it can also facilitate the rapid transfer of information between jihadist groups and pass on information that the center has gathered. In this way, the online representatives of jihadist groups can then pass the information on to the leaders of these groups via courier, even in the remote areas of the Northwest Frontier Province in Pakistan.

This mechanism may help explain how isolated jihadists like bin Laden and Zawahiri can reference extremely current events in the propaganda they release. Likewise, the efficiency of Al-Fajr Center may also explain how jihadist leaders have been able to release messages more frequently than in the past. Reinforcing this trend is that jihadist leaders have begun to release their videos online first, rather than relying on the al-Jazeera television network, which often only shows a small portion of the entire propaganda piece.

Al-Fajr Center is a powerful tool for jihadist groups because their messages can be spread rapidly while retaining their authenticity. As the primary outlet for most of the major jihadist groups, Al-Fajr Center's operations contribute greatly to fostering a unified, global jihadist community. Similarly, the center benefits jihadist groups themselves by allowing them to coordinate, share information, and consolidate their power to continue to lead the jihadist movement. Damaging Al-Fajr Center would prove a severe blow to the jihadist groups' ability to gather information, proselytize, and recruit.

From Propaganda Groups to Terrorist Facilitators

While some may think that propaganda groups like Al-Fajr Center are not an immediate threat because they only release propaganda on the internet, the reality is that the propaganda groups themselves facilitate terrorist activity. A case in point is the Global Islamic Media Front (GIMF), one of the oldest and most prominent virtual propaganda groups. The GIMF, which also disseminates its propaganda through Al-Fajr Center, is just one of many virtual groups who contribute propaganda to the online jihadist community. Some groups, like GIMF, do not work for any one particular jihadist organization but are instead made up of supporters who believe in the jihadist ideology and support the general movement. The existence of these groups provides the online jihadist with a continuous stream of propaganda, never leaving the online jihadist community without movies, documents, messages, magazines, training manuals, and even video games, all of which are created to indoctrinate others to support the jihadist cause.

GIMF, which openly supports al-Qaeda, produces copious amounts of propaganda maintains a hidden membership of individuals scattered throughout the world. These ardently dedicated individuals produce a wide variety of jihadist propaganda in the form of Flash presentations,



videos, online television news, and even video games. One of GIMF's most popular video games was titled "Night of Bush Capturing." The first-person perspective shooting game, in which the player targets American soldiers, President George Bush, Prime Minister Tony Blair, and Grand Ayatollah Ali Al-Sistani, was distributed in September 2006 throughout jihadist message boards and created for "terrorist children."

However, GIMF's activities were not limited to propaganda; instead, many of its members plotted terrorist attacks themselves, using the virtual network they had built to facilitate its actions. In the summer of 2007, Mohammad Mahmoud, a leading member of GIMF living in Vienna, Austria, worked closely with Jeish al-Islam, the Palestinian jihadist group responsible for the kidnapping of BBC journalist Alan Johnston in the Gaza Strip. In this case, Mahmoud used his online network to help the terrorist group issue statements and parade the powerful symbol of a Western hostage.

Soon, however, Mahmoud took further steps to help others plan attacks. Known on the internet as "Gharib al-Diyar," Mahmoud ran the German-branch of GIMF, but did not limit himself to propaganda only. In 2003, he travelled to Iraq to attend a training camp run by Ansar al-Islam, a jihadist group currently active in Iraq under the name Ansar al-Sunnah. After producing a March 2007 GIMF video speech threatening attacks in Germany and Austria, Mahmoud composed a rough message outlining several physical targets to attack, specifically the Euro 2008 football championships in Austria and Switzerland, OPEC's Vienna-based headquarters, as well as UN buildings in Vienna and Geneva.

In September 2007, officials in Vienna arrested Mahmoud and two of his associates, while a coordinated arrest took place outside Montreal, Quebec, in which Canadian officials arrested Said Namouh. According to a charge sheet filed in Quebec, Namouh conspired with Mahmoud "for the purpose of delivering, placing, discharging or detonating an explosive in a place outside Canada." Using the name "Achrafe" on the internet, Namouh was also an important member of GIMF, sending hundreds of messages to other members of the group all over the world. Notably, the internet enabled Mahmoud to provide Namouh with the alleged support to plan a terrorist attack while across the Atlantic Ocean.

As this example demonstrates, jihadist propaganda groups must also be treated as potential terrorist cells. This GIMF case is but one example of many other cases where those facilitating propaganda seek to support actual attacks. Indeed, instructional manuals produced by virtual jihadist groups like GIMF now encourage individual jihadists and jihadist groups to train as multi-faceted operators, learning both the production and dissemination of media propaganda in addition to the technical operations required to carry out attacks. As this trend continues, it becomes increasingly dangerous to view individuals involved in jihadist propaganda as disconnected from those seeking to carry out attacks. It is therefore extremely important that we closely monitor virtual jihadist groups, no matter how small, to learn as much as we can about them and their activities before they are able to cause harm.



The Virtual Jihadist Network

Jihadist groups use the internet to provide a virtual social network to indoctrinate, recruit, and train followers. Because of the constant and overwhelming propaganda the jihadists produce, any individual, even with no prior association to jihadist ideology, can quickly feel like he or she is part of the global jihadist community and self-radicalize himself or herself. Once a believer, these self-radicalized individuals will seek out others who think like them online, eventually discovering the primary source jihadist websites run by the jihadists themselves. By studying these primary source websites, jihadist groups can cull new recruits while exerting much less effort, as potential recruits come to them, rather than the opposite.

In addition, through this virtual jihadist network, jihadist groups can indoctrinate individuals and then provide them with the tools they need to carry out either individual or small group attacks, without having to be specifically recruited by an established jihadist group. Jihadists provide strategies and tactics for the entire community so that independent terrorist cells can spring up throughout the world. From online training manuals, these independent cells can learn which are the best targets to attack, how to attack them, and how to make sure that the attack will be inline with the overall jihadist strategy.

The virtual jihadist network revolves around these dimensions:

- Recruitment
- Propaganda, Indoctrination, and Psychological Warfare
- Training and Tactics
- Communication and Coordination
- Strategy
- Financing

The following will examine each dimension of the virtual social network in further detail.

Recruitment

Recruitment takes on two forms in the online jihadist community. The first path is attempting to head to a current theater of conflict to fight with the mujahideen. These recruits are sometimes required to bring money with them to support the jihad. Though many jihadists likely utilize local connections to make their way to the lands of jihad, online handlers also exist to aid jihadists wishing to travel to an area where they can fight. Mark Robert Walker, a 19-year-old student in Laramie, Wyoming, originally from Rochester, New York, pled guilty to aiding a terrorist organization in October 2005. Using the screen name “Abdullah,” Walker was in contact with an online individual named “Khalid” who had agreed to help Walker leave the United States to fight with jihadists in Somalia. The FBI intercepted Walker’s online communications with “Khalid” and arrested Walker at El Paso International Airport, as he attempted to leave the country.



Walker's case is not isolated; many like him exist within the online community. These members who desire to travel to lands of jihad to fight with the mujahideen are reinforced by the material found on the forums. Jihadist messageboards proudly announce when a member of a forum has been killed while fighting. On February 6, 2007, the al-Hesbah jihadist forum carried a message announcing that one of its members had carried out a successful suicide attack in Iraq that "shook the crusaders" in Iraq. The individual, an established jihadist online figure known by the alias "Risalah," died while fighting since the start of 2007. On January 3rd, 2007, Na'im Muhammad bin Abdullah, also a member, was announced to have been killed fighting U.S. forces in Baghdad. Both were prominent members of the online jihadist community. The announcements of their deaths prompted praise from other members, reinforcing the strength of the community. This praise also paints physical jihad as a natural outgrowth of participation in the online forum.

Al-Hesbah is not the only jihadist forum with members who have left to join the jihad. For example, after a Saudi administrator of the Hedayah forum² was killed fighting in Iraq in December 2006, one member eulogized him, "In the forum he was special and was a provider . . . and there he is today, writing . . . with his blood, not with his pen." Just traveling to a land of jihad garners praise, as well. In December 2006, it was announced that Firas al-Ta'an, a moderator of Al-Ekhlaas³ jihadist forum, had traveled to Iraq and reached the mujahideen safely.

Rather than travel to where there is active fighting, the other path a recruit can take is to engage in a local terrorist plot, where no handler is needed. Instead, the training manuals, tactics, and strategies available within the online jihadist community take the place of a handler. For example, in March 2004, Mohammad Zaki Amawi, a US citizen, returned to Ohio after a failed attempt to enter Iraq through Jordan to fight against US and coalition forces. Undeterred by his inability join an active front, Amawi gather jihadist training manuals and videos through jihadist websites to build his own cell in Toledo. He soon recruited others local to the area.

Among the materials Amawi collected from online sources to train the cell were a "Basic Training" course for jihadists, a prerequisite for an "Advanced Training" course, videos on the production and use of improvised explosive devices (IEDs), and an instructional video for building a suicide bomb vest, titled "Martyrdom Operation Vest Preparation." One member of the cell, Marwan Othman El-Hindi, proposed downloading the videos to show to two of his recruits in Chicago. For practice, the cell traveled together to a shooting range in Toledo. During this time, Amawi maintained contact with jihadists traveling into and out of Iraq using encrypted e-mail messages, contacting them for technical assistance.

These self-starting cells can also span continents. While in England, Younis Tsouli, the online jihadist known as Irhabi007, was in contact with two men from Atlanta, Georgia, who were providing Irhabi007 with surveillance videos of American targets. The men, Ehsanul Islam

² <http://www.hedaaya.net>

³ <http://www.alekhlaas.net/>



Sadequee and Syed Haris Ahmed, visited Washington, DC, and recorded video footage of the U.S Capitol, the Masonic Temple, the World Bank, and a fuel depot. Their footage was found amongst Irhabi007's belongings.

This cell, however, also had another component connected through the internet. In June 2006, Canadian authorities disrupted the cell in Ontario, arresting 17 individuals, including 5 minors. Many members of this cell are charged with attempting to blow up targets throughout Canada. It was soon revealed that the two Georgian men providing support to Irhabi007 had traveled to Canada to meet with members of the cell, after having met online. The men from Georgia were also members of the same jihadist messageboard as some of the members of an alleged cell in Canada.

Jihadists will continue to utilize the internet to recruit others to plan attacks so long as the internet remains a safe haven. Recruitment takes place on jihadist forums in many languages, from Arabic to German to English. By infiltrating the jihadists' online forums, we can better monitor the relationships between online jihadists, looking for both those who wish to travel to lands of jihad as well as those seeking to do harm locally. Studying messageboards allows us to determine which online jihadists participate in the recruiting process and enables us to develop countermeasures to act against them. Furthermore, identifying the physical locations of online jihadists can disrupt actual cells and prevent actual attacks.

Propaganda, Indoctrination, and Psychological Warfare

The propaganda the jihadists release is powerful and reaches a global audience. As one jihadist recalled, "The first time I saw an al-Qaeda video, I was ready to go. I wanted to kill the disbelievers."⁴ The propaganda in jihadist videos is compelling, convincing, and able to be accessed in a growing number of languages. While most primary source propaganda is released in Arabic, individuals and groups dedicated to the jihadist cause will translate them into their vernacular language, so that the message of jihadist leaders can be heard across the world.

⁴ Stewart Bell. "Making of a Zealot." *National Post*. June 30, 2006.



Jihadist propaganda is released in English, Turkish, French, Somali, Russian, and a host of other languages. Jihadist messageboards and websites also exist exclusively in English and other languages as well. Even some extremely prominent Arabic jihadist messageboards, like the Al-Hesbah⁵ forum, now contain an English section. Because of the availability of jihadist propaganda in so many languages, potential jihadists can know only their native language and still be radicalized.

By being able to reach a global audience, jihadist groups can continue to indoctrinate many more individuals than they could otherwise without a propaganda outlet through the internet. In an interview released in December 2005, Zawahiri explicitly discussed al-Qaeda's policy of distributing important videos and messages as widely as possible. At the conclusion of the 43 minute interview, Zawahiri calls upon media organizations to distribute the interview in "all languages and as widely as possible." The release of the interview itself carried English subtitles and was distributed shortly thereafter with French, German, and Italian subtitles on online forums by December 2005.

In the last year, al-Qaeda's production company, As-Sahab, has begun to produce English transcripts and subtitles for most of al-Qaeda's major releases, especially messages from bin Laden and Zawahiri. In the past year, at least 20 videos from As-Sahab have been released with either English subtitles or transcripts, broadening the group's reach. Al-Qaeda has also issued videos in English speaking directly to Americans. A native Californian wanted by the FBI for his role in al-Qaeda, Adam Gadahn, or Azzam al-Amriki, provides a voice directly from the al-Qaeda leadership in Afghanistan to the American people. His September 2006 video, "An Invitation to Islam," carried the messages of al-Qaeda but in an American accent. Gadahn devoted much of his 45 minute video to explaining al-Qaeda's ideology, rationale, and motivations.

While Adam Gadahn speaks to an American audience, al-Qaeda uses the British men who perpetrated the July 7, 2005, bombings in London. In commemoration of the bombings, an annual video is released to the forums in which one of the bombers discusses his reasons for the attack in a thick Yorkshire accent. As with "An Invitation to Islam," each of the 7/7 commemoration videos are edited as compilations combining clips of al-Qaeda leadership with a significant portion read by a native speaker to the people of the country being addressed.

The demand for jihadist materials in other languages is high. Recently, an influential French jihadist forums, al-Mourabitoune⁶, has begun providing translations of videos and statements of responsibility from Arabic into French with very little lag time. For example, on May 23, 2006, GIMF released bin Laden's "A Testimony to the Truth" with both Arabic and English transcripts. By the next day, al-Mourabitoune was carrying a French translation of the transcript. Following a flood of requests posted to English and French messageboards, GIMF provided subtitled editions

⁵ <http://www.alhesbah.org>

⁶ <http://www.ribaat.org>



of Abu Musab al-Zarqawi's April 26, 2006, video, entitled, "A Message to the People." A version of "A Message to the People" with French subtitles was soon released along with a full French transcript to French-language jihadist forums on May 4, 2006.

While many may perceive jihadist propaganda as crude and barbaric, replete with beheadings and bombs, much propaganda is instead strongly argued rhetoric that is becoming increasingly sophisticated. Jihadist ideologues, like Hamid Al-Ali in Kuwait, release masterful pieces of religious rhetoric exhorting others to jihad. Many of the white papers, studies, books, and other documents that the jihadists release are heavily footnoted and maintain a scholarly tone. The result is that the propaganda takes on an air of professionalism and scholarship that is extremely convincing to critically thinking potential jihadists.

Oftentimes jihadist ideologues appeal to baser emotional responses to violence and sex. Abu Musab al-Zarqawi's filmed beheadings attracted an instant audience, and videos are released daily of attacks, gruesome shots of dead victims and mujahideen, and other gore. This gore serves as powerful psychological warfare, and sensationalized murders, like beheadings, intimidate the enemies of the jihadists while bolstering jihadist support. On the other hand, the death of mujahideen is portrayed as painless, desensitizing many to the fear of participating in such violence.

While not commonly addressed, sometimes sex is exploited to attract jihadists. In November 2006, a three and a half minute audio message from Hamid Al-Ali, an extremely important jihadist shaykh famous for his fatwas and designated a terrorist by the United States, was posted to jihadist messageboards explaining the great rewards in heaven waiting for those who die in battle. The speaker provides strikingly erotic details about the "wives" which pleasure martyrs in paradise:

"Paradise has eight great gates through which whoever enters will never come out again. Each gate determines what the martyr has achieved; in Paradise they will enjoy endless tasteful food and drinks, with a beloved wife. She will astonish your mind. Her hair is made of silk. Her flirtation appears in the bed as politeness and expertise in these things; she knows all about sexual intercourse. By touching, looking, and hearing, her vagina never complains about how much sex she had. She becomes a beautiful virgin again. The more intercourse she has the more love she gives, and she gives a beautiful smile."⁷

The amount of propaganda the jihadists produce is staggering. With jihadist propaganda widely available in numerous languages, the jihadists can reach an extremely large audience. This large reach of jihadist propaganda, coupled with the shrewd use of rhetoric, has created an online jihadist environment where individuals are capable of self-radicalizing themselves with little

⁷ Hamid Al-Ali. "Description of Martyrs in Paradise." Audio clip circulated on jihadist forums and posted on Hamid Al-Ali's official website at http://www.h-alali.info/snd_open.php?id=b75e9fb4-f2b5-1029-a701-0010dc91cf69



direct guidance from established jihadist groups. So long as this propaganda is not countered, jihadists will always have a steady stream of potential recruits.

Training and Tactics

Using the internet, jihadists have created a virtual classroom that teaches the online jihadist community how to produce and construct weapons ranging from simple IEDs to nuclear, biological, and chemical weapons. Not only are jihadists taught military tactics; they also learn how to mine the internet for information, protect their anonymity online, encrypt the contents of their computers, and use the internet to benefit the global jihadist movement. Given the difficulty many individuals have in reaching training camps in the post-9/11 world, online training gives jihadists the tools they need to plan, coordinate, and execute terrorist attacks. Indeed, soldiers from Iraq have informed us that training manuals discovered in jihadist safe houses in Iraq were printed from the jihadist manuals found online.

Al-Qaeda and other jihadist groups have produced magazines and multimedia exclusively for training purposes. “Al-Battar,” a publication of al-Qaeda in Saudi Arabia, is solely dedicated to training prospective mujahideen, even supplying ideal targets. Issues have featured weapons discussion, such as using a pistol for sniper training, how to hold and target a rocket-propelled grenade (RPG), and survival tactics. Even though the most recent issue of “Al-Battar” was released two years ago, the magazine continues to widely circulate online on jihadist websites.

Excerpts from large compendiums of urban warfare, explosives and poisons training manuals are frequently posted to the jihadist forums, in addition to members own suggestions, often using photographs and video to support their explanations. Videos exist which give training instructions for suicide bombings, construction and dismantling of landmines, and composition of various explosives substances. Electronic books, or e-books, are also used to provide a single resource for particular training. For example, an e-book compilation of IED construction, camouflage, and placement was distributed to the password-protected al-Firdaws⁸ forum, which contains a special military section. This publication suggested the planting of explosives in shopping bags in markets, butter tubs, flower bouquets, candy boxes, briefcases, and buses.

In addition to traditional explosives, jihadists are also attempting to educate themselves about chemical, biological, radiological, and nuclear (CBRN) weapons, which are incessantly discussed on jihadist forums. The “Encyclopedia of Poisons” offers a variety of methods to kill an enemy with a several toxic substances and is freely available to any member of the online jihadist community. Ricin and botulism bacilli are just two examples of individual poisons that have received much attention on jihadist forums. Members on these forums detail the speed with which a victim will die when receiving the poisons by injection, inhalation, or digestion. Other weapons of mass destruction, including nuclear and radiological devices have also been the subject of interest and instruction by the jihadists. One author, calling himself “Ozoo”,

⁸

<http://www.alfirdaws.org>



produced a large compendium offering nuclear knowledge among other security, espionage, and military training.

In addition to physical preparation and military training manuals, the jihadists also impart knowledge to each about computer technology. Internet anonymity, of primary importance to members to avoid surveillance and capture, is frequently addressed. Al-Fajr Center, GIMF, and other jihadist media groups release cybersecurity manuals to aid the online jihadists. Al-Fajr Center created a specific cybersecurity magazine, “Technical Mujahid,” which provides information remain anonymous online, how to utilize Pretty Good Privacy (PGP) software for encrypted communications, and detailed methods for a user to hide their sensitive files using a virtual machine. In its first pages, the “Technical Mujahid” states the jihadist stance concerning the virtual battle ground: “the internet provides a golden opportunity... for the mujahideen to break the siege placed upon them by the media of the crusaders and their followers in the Muslim countries, and to use [the internet] for [the sake of] jihad and the victory of the faith.” The GIMF provides similar information and recently distributed an encryption program built by the jihadists themselves to facilitate anonymous communications.

Tactical information is rapidly shared on jihadist messageboards. They study our analyses, distribute our reports, and quote our editorials, searching for our weaknesses. On their own initiative, jihadists are constantly providing data to the forums, posting maps of suggested targets, locations of American bases throughout the Middle East, and distributing aerial photographs captured by the Google Earth software, while others pull maps from government and university libraries.

Several primary jihadist websites house areas solely dedicated to training. Within these training areas, jihadists are encouraged to contribute their own expertise and data, so that all the jihadists can benefit from the knowledge of the entire jihadist community. Indeed, some of these forums even hold online training seminars, where less experienced jihadists can ask questions to jihadist weapons experts and receive direct responses online. In this manner, should any jihadist have difficulty in successfully manufacturing a bomb, or has a question regarding the procurement of required ingredients, there are thousands of other members, some with significant experience, who are available to provide the desired information.

By studying the training manuals and tactical material that exist on jihadist messageboards, warfighters can understand better the types of weapons likely to be used against them as well as the targets that jihadists are choosing for attack. Additionally, observing the training jihadists receive online will help security officials plan for threats discussed on jihadist websites, eliminating some of the guesswork involved in imagining the types of attacks jihadists are planning. While finding and destroying physical training camps will be essential to prevent jihadists from learning how to attack us, jihadists can instead rely on the internet for an interactive, comprehensive military education.



Online Communication and Coordination

Due to the efforts of security forces around the world, jihadists have an increasingly difficult time communicating and coordinating with one another utilizing traditional communication devices that can be easily traced, such as cellular or satellite phones. However, the internet provides a flexible, instant communication tools for jihadists. Whether via email, chat rooms, instant messaging services, e-groups, messageboards, websites, or voice over IP (VOIP), jihadists can communicate securely with one another rapidly using sophisticated, freely available encryption methods.

Jihadist media groups like GIMF and Al-Fajr Center release programs and training manuals to ensure that members of the online jihadist community know how to communicate with each other securely, using encryption methods like PGP. Groups and individuals desiring to form their own cells can therefore coordinate online with each other clandestinely below the radar of security officials. Even individuals spread across vast geographic areas can communicate with one another instantly and securely, forming virtual cells that work together. The members of these virtual cells may never meet each other in person but can nevertheless aid one another in planning attacks.

Established jihadist groups like al-Qaeda can also communicate online to discuss everything from strategy to attacks. In one telling example, in December 2005, a top jihadist ideologue using the pseudonym Louis Attiyah Allah wrote to Abu Musab al-Zarqawi, discussing Zarqawi's role in Iraq and its place within the larger jihadist movement. At the end of the letter, Attiyah Allah notes to Zarqawi that he can be contacted on the "Ana Al-Muslim"⁹ jihadist forum, indicating that even the top leadership of al-Qaeda uses the internet to communicate.

As one notable example of cross-continental coordination, the infamous online jihadist Irhabi007, whose real name is Younis Tsouli, was arrested in England in October 2005 and was indicted under the UK's Terrorism Act 2000, with charges including "conspiracy to murder, conspiracy to cause an explosion, conspiracy to obtain money by deception, fundraising and possession of articles for terrorist purposes." Tsouli gained fame online for his teaching the global jihadist movement hacking and cybersecurity skills while facilitated the dissemination of jihadist propaganda coming from jihadist groups in Iraq and elsewhere.

As part of his online activities, Tsouli was also in communication with a jihadist cell in the United States. In March 2006, two Americans in Atlanta, Georgia, were arrested and eventually charged with "material support" to a terrorist group and are accused of plotting to attack oil refineries in the United States. These men, Ehsanul Islam Sadequee and Syed Haris Ahmed, visited Washington, DC, in spring 2005 and recorded video footage of the U.S Capitol, the Masonic Temple, the World Bank, and a fuel depot. Remarkably, this footage was also found among Tsouli's belongings, indicating that the two American terror suspects were indeed in

⁹

<http://www.muslm.net>



contact with Tsouli and were feeding him tactical information via the internet.

Aside from the obvious means by which small cells can coordinate and plan attacks through the internet, the online jihadist community has also engaged in coordinated cyberattacks on numerous websites. Because the jihadists can freely communicate while online, jihadists can designate electronic targets to a widespread audience and establish common timetables to launch cyberattacks. The electronic attacks usually involve “Denial of Service” (DoS) attacks whereby a targeted website is flooded with requests at a single time. For these attacks to be successful, numerous individuals must attempt to access a website simultaneously.

Because the internet provides the jihadists a means to advertise the timing of a DoS attack to a large number of jihadists in a short time, these types of attacks only fail when too few jihadists participate in the attack at the same time. Prominent members of the jihadist Internet community, such as Irhabi007, have instructed jihadists in how to execute DoS attacks, and some groups that have announced a planned attack provide the necessary software with the address of the target already inputted. This method of attacking the enemy allows online jihadists to target Western interests from their own home and with little risk.

The results of these hacking initiatives have resulted in breaches of government security. Jihadists have hacked government and military websites and have retrieved extremely sensitive information on soldiers, including their areas of deployment, their health status, their social security numbers, their salary, their bank accounts, and other demographic information.

Jihadist cyberattacks launched on Dutch websites, including those belonging to the Dutch government, in January and February 2006 took many offline. The DoS operation, results, and images of a dead Theo van Gogh, a Dutch filmmaker who was murdered by a jihadist, were included in a video distributed shortly celebrating the attack. In another case, on November 27, 2006, a message was distributed on jihadist forums announcing the “Electronic Battle of Guantanamo,” which was to target the websites of American stock exchanges and banks. The Department of Homeland Security warned about the attack and its danger, and though nothing came of the electronic jihadist operation, it fueled the desire for additional attacks. Even the Vatican’s website was targeted by jihadists.

Retarding the ability of jihadists’ to communicate is another necessary step in minimizing the jihadist threat. Though governments have done well in preventing jihadists from utilizing traditional means of communication, the internet remains the best communication device for the entire jihadist community. Allowing them to communicate instantly over vast distances, virtual cells can form quite easily, and coordinating cyberattacks requires a mere posting to a messageboard announcing the time and date of such attack.

While obviously we can never shut down the internet, we can monitor jihadists’ use of the internet and track down their physical locations. Once jihadists learn that the internet is not a safe haven for their communications, many will become fearful of utilizing the internet as a means to communicate. It is unlikely that we will ever cut jihadist communication online to



nothing, but at the very least, we can provide disincentives to jihadists using the internet by punishing those who do.

Strategy

The strategy behind the jihadist movement is not amorphous. Jihadist ideologues have developed a timeframe for their jihad, thinking both short-term and long-term, and understanding that success will only come after years of struggle. Major jihadist ideologues are able to direct the global jihadist movement by releasing white papers and books analyzing the situation of the jihadist movement and providing the jihadists with long-term strategies to ensure that the movement itself always has directions and goals. Jihadist strategies are released online and are widely circulated on jihadist forums so that the entire jihadist community can follow the same strategies and goals, reducing the discord amongst them.

One of al-Qaeda's most important strategists subsequent to 9/11 is Abu Musab al-Suri, an al-Qaeda operative who ran terrorist training camps in Afghanistan. Al-Suri's publications and studies are highly regarded by jihadists and are always housed on primary source jihadist websites and others. His 1600-page magnum opus, "The Global Islamic Call to Resistance," is an extremely influential jihadist manifesto and is available to download in a variety of digital formats. Jihadists discuss and analyze Al-Suri's writings both publicly and secretly to understand, develop, and expand upon his ideas.

In "The Global Islamic Call to Resistance," Abu Musab al-Suri details his theories of how to best wage jihad in the twenty-first century. The scope of the book is very broad, with topics ranging from a history of the Islamic world to autobiographical anecdotes about his role in the jihadist movement. However, a significant portion of the book discusses the most effective strategies for waging jihad against the West. Focusing on the types of attacks that will bring the mujahideen the most success, al-Suri advocates establishing self-starting, independent cells in Western countries with no direct affiliations to established jihadist groups. These cells operate to support the global jihadist movement, rather than any particular organization or leader.

Many of al-Suri's publications reiterate that jihadists must set up independent cells within their country of residence, bide their time, and only strike when the time is appropriate. Better, al-Suri intimates, to wait ten years studying and planning for a large, poignant attack rather than carry out a quick suicide bombing at a mall in America doing little damage. Al-Suri was arrested late 2005, yet, demonstrating the power of the internet, his strategies and theories continue to exist in cyberspace. Al-Suri's videotaped lectures at Al-Ghurabaa training camp in Afghanistan prior to 9/11 have been digitized and are available online as well. Whether dead or captured, the internet provides jihadists with a virtual immortality.

Available online, the publications of al-Suri and other ideologues share common themes in their strategies. These strategies include:



- Utilizing guerilla warfare
- Establishing self-starting, independent cells in Western countries with no direct affiliations to established jihadist groups
- Damaging the United States' economy through terrorist activities
- Attacking Arab governments that work closely with the West
- Attacking Western targets in Arab countries.

These strategies also include specific targets. For example, Al-Suri organizes the most important targets to attack in America and its allies as follows:

- Politicians
- Major economic targets, like the stock exchange, airports, bridges, metros, tourist attractions
- Military bases
- Media personalities
- Computers and information centers that connect the institutions of the country
- Jewish gatherings and notable Jews
- The offices of supranational targets, like NATO and the EU
- Buildings belonging to the CIA, FBI, and other security institutions
- Civilians, while avoiding women and children if possible, to prevent generating negative publicity

Obviously, these targets are not the only vulnerable individuals and institutions in the West. However, by studying and understanding the strategy the jihadist ideologues propose, we can better prepare ourselves against attacks that independent jihadist cells are likely to target. Also, we can develop more effective long-term counterstrategies against jihadists once we discern how they plan on expanding the jihadist movement. Therefore, the need to study jihadist strategies on the internet is paramount; it is an open window showing us how the jihadist movement will likely develop in the future.

Financing

Stemming the flow of money to jihadists is essential. Though carrying out terrorist attacks usually requires relative little money, jihadists do need funding for weapons, training, distributing propaganda, and the costs of hosting internet websites and messageboards. Since 9/11, the US, the UN, and other countries have worked hard to locate the methods and means by which terrorists transfer money. Prior to this crackdown, money was transferred to terrorist groups through sham front groups and charities or through offshore banking techniques. The US and others had much success in identifying the financiers of terrorism and exposing them.

While these traditional techniques no doubt still play a role in terrorist financing, jihadists have also turned to using the internet to transmit funds. Online remittance systems and other means of



transferring money over the internet are constantly being used by jihadists to finance the jihadist movement. Jihadist webmasters use these electronic means to pay for their servers, and virtual jihadist groups have now appeared online soliciting donations from followers.

The Islamic Army of Iraq, an insurgent group operating within Iraq, released a video celebrating its October 15 attack on an American ammunition facility in Baghdad. Interestingly, this video ended with a plea for donations to be sent to “The Electronic Nusra Society.” Two days later, the group released the tenth issue of its online magazine, “Al-Forsan,” which contained a full page advertisement seeking donations for the “The Digital Nusra Society.” Though these advertisements offered no physical address to which to send donations, they indicated that donors could contact the group electronically for further instructions on how to donate.

Discussions on jihadist messageboards have gone into specific detail explaining how jihadists can donate online to jihadist groups. On the influential Al-Hesbah online forum, one jihadist described the process by which cash can be transferred through online remittance services. With certain online remittance services, individuals can add money to their online bank accounts by using cash to purchase physical cards (similar to phone cards) of various values from designated “brick and mortar” retailers across the world.

Using such an online bank account, an individual could then transfer cash to a jihadist group in the following manner:

1. The individual wishing to send jihadist groups cash purchases a physical bank card and transfers the value to an intermediary jihadist via an email with the required information to transfer the money.
2. The intermediary jihadist, in direct contact with the mujahideen, receives the online money transfer and then gives the mujahideen the value of the transfer in cash.
3. The jihadist groups receiving the cash from the intermediary can use the funds however they like, while the intermediary jihadist who received the initial online money transfer can use that money to purchase online goods.

As an example, a donor could purchase \$100 worth of online virtual money from a physical store and then email the value of that money to an intermediary jihadist. That intermediary, now \$100 richer, will give a jihadist group \$100 in cash out of his own pocket. The intermediary, however, now has \$100 worth of virtual money to spend online, while the jihadist group now has \$100 in cash.

While this type of remittance is just developing and is only one way of transferring money, the chatter surrounding the ways to transfer money through the internet has been increasing on jihadist messageboards. Discovering and monitoring how jihadists transfer money online will enable us to further act against their financing methods, as we have done successfully before with traditional remittance services. If we are to continue our assault on terrorism financing, authorities must devise new ways to monitor and regulate online remittance services that can be abused by jihadists.



Conclusions

The internet remains one of the most valuable tools the jihadists have at their disposal, serving all the functions necessary to sustain a violent jihadist movement at minimal cost. Through virtual means, jihadists have in many ways replaced the training camps of the 1980s and 1990s that jihadist groups established in Afghanistan and elsewhere. Indoctrination, recruitment, financing, and training continue 24 hours a day on jihadist messageboards. A National Intelligence Estimate (NIE) Report produced in April 2006 and declassified in September 2006 agreed, “We judge that groups of all stripes will increasingly use the Internet to communicate, propagandize, recruit, train, and obtain logistical and financial support.”¹⁰

In recent years, many have realized the extraordinary power that jihadists obtain by being able to exploit the internet. However, little seems to have been accomplished in preventing jihadists from using the internet to their advantage, directly harming our security, both domestic and foreign.

As long as the internet remains an uncontested safe haven for jihadists, the jihadist movement will continue to grow, regardless of the death or arrest of any jihadist leader or ideologue. The internet provides immortality to the ideology behind the jihadist movement, and countless individuals can absorb this propaganda, which is readily available in numerous languages. While not all individuals exposed to jihadist propaganda will succumb to it, the images, sounds, and thoughts that the jihadists produce are carefully woven, attractive, and compelling. Many will buy into the ideology and become part of the online jihadist community. So long as this virtual community exists unopposed, jihadist groups will always be able to refill their ranks and keep their movement alive, indoctrinating and training their future army.

The challenge now is to infiltrate and erode this virtual network to weaken this driving force behind the global jihadist movement. Studying the online jihadist community empowers us. We can listen to what they say, understand the way they think, and determine how they operate. We can grasp their ideology and devise effective counter-propaganda. We can better defend known targets, identify potential threats, devise countermeasures to their tactics, undermine their strengths, and exploit their weaknesses. There is a wealth of information available online, if we

¹⁰ http://odni.gov/press_releases/Declassified_NIE_Key_Judgments.pdf



are willing to take the time to collect, study, and analyze the data.

To take advantage of this online intelligence and counter the jihadists on the internet, policy makers and authorities should embark on the following steps:

1. Understand how jihadists utilize the internet, including the hierarchy and structure of online jihadist networks, the technical process of distributing the videos, and how jihadists exploit services on the internet.
2. Effectively monitor jihadist activity on the internet. Because monitoring the entire internet is impossible, understanding the hierarchy of online jihadist networks will help focus efforts on the most important websites and other internet services the jihadists use.
3. Identify and exploit the weaknesses of the jihadists on the internet.
4. Mine jihadist activity on the internet for intelligence. By successfully infiltrating the most important jihadist forums, more specific, actionable intelligence can be obtained than simply by monitoring secondary and tertiary jihadist websites. This intelligence can then be used to deal severe blows to the global jihadist movement.

For as long as jihadists on the internet can engage in terrorist activities unfettered and unmonitored, the U.S. will not be able to cause significant, lasting damage to the global jihadist movement. The internet plays a key role in fostering homegrown radicals, providing them with all the information necessary to conduct local attacks as well as a location to meet and plan without being detected easily. If the global jihadist threat, both domestic and abroad, is to be combated effectively, the U.S. must invest significant resources into studying, monitoring, and understanding how jihadists utilize and exploit the internet.